REMARKS

Introduction

This Reply is in response to the Office Action of June 11, 2009. Reconsideration of this application in view of the following remarks is respectfully requested.

The §101 Rejections

Claims 1-19 were rejected under 35 U.S.C. §101. It was suggested that claims 1-19 were directed towards mental steps that can be implemented without a computer. Independent claims 1, 13, and 18 have therefore been amended to make it clearer that the methods of claim 1, 13, and 18 are tied to computing equipment. Claims 1-19 are therefore patentable under 35 U.S.C. §101.

The Prior Art Rejections

In the Office Action, claims 1-12 and 18-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zheng U.S. Patent No. 6,396,928 in view of Boneh et al. U.S. Patent No. 7,113,594. Claims 13-17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zhen in view of Rohatgi U.S. Patent No. 6,826,687. These rejections are respectfully traversed.

Claims 13-17

Claim 13 is directed to a method of signing and encrypting a message M in which an IBE private key is used to compute a commitment to a secret value and a corresponding decommitment and in which a symmetric key that is based on the IBE private key is used to encrypt at least one of the commitment and the decommitment.

In the rejection of claim 13, it was conceded that Zheng does not disclose using an IBE private key to compute a commitment to a secret value and a corresponding decommitment. In spite of this admission of Zhang's deficiency, it was still suggested that Zheng discloses using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment (both of which Zheng admittedly does not even compute).

However, there is nothing in Zheng that shows or suggests even a symmetric key that is based on an IBE private key. In particular, the cited portions of Zheng (FIGS. 3 and 4 and col. 13 lines 34-67) describe a random message-encryption key k and, for each recipient i, a transmission key t_i calculated from a random number v_i and the recipient's public key y_i (specifically, $t_i = y_i^{v_i}$). Zheng simply does not show or suggest using a symmetric key that is based on an IBE private key to encrypt anything, let alone to encrypt at least one of the

commitment and the decommitment (again, both of which Zheng admittedly does not even compute).

Rohatgi was suggested to disclose using an IBE private key to compute a commitment to a secret value and a corresponding decommitment. However, like Zheng, Rohatgi fails to show or suggest using a symmetric key that is based on an IBE private key to encrypt at least one of the commitment and the decommitment.

Regardless of whether or not Rohatgi discloses using an IBE private key to compute a commitment to a secret value and a corresponding decommitment (as suggested in the Office Action), Rohatgi and Zheng both fail to show or suggest using a symmetric key that is based on an IBE private key to encrypt at least one of the commitment and the decommitment, as required by claim 13. Claim 13 is therefore patentable over Zheng and Rohatgi, whether or not these references are combined as proposed in the Office Action. Claims 14-17 depend from claim 13 and are patentable because claim 13 is patentable.

Claims 1-12 and 18-19

Claims 1 and 18 are directed to identity-based-encryption signcryption methods in which decrypting a ciphertext produces an IBE public key of the sender ID_A. Both claims 1 and 18 require that decrypting the ciphertext produces an IBE public

key of the sender ID_A that corresponds to the IBE private key SK_A.

In the rejection of claim 1, it was conceded that Zheng fails to show or suggest that decrypting ciphertext produces an IBE public key of the sender ID_A that corresponds to an IBE private key SK_A of claims 1 and 18. It was suggested that Boneh makes up for the deficiencies of Zheng. Col. 8, lines 29-35, col. 24, line 52 to col. 25, line 18, and col. 25, lines 50-65 of Boneh were cited as being relevant.

Col. 8, lines 29-35 of Boneh disclose that a public identifier ID can contain a character string known to the public to be associated with a particular entity and can, in general, be any arbitrary piece of information. Enhanced identifiers that contain information not limited to information specifying the identity of a particular entity may also be used.

Col. 24, line 52 to col. 25, line 18 of Boneh describe a t-out-of-n distributed private key generator arrangement. In this arrangement, multiple private key generators each have a share s_i of a secret s (i.e., a user's private key). Users can construct an entire private key from a plurality of shares of the private key as long as they have a minimum number of shares of the private key (i.e., t shares from n different private key generators).

Col. 25, lines 50-65 describe that a receiver may

queries two of three (i.e., t of n) private key generators using the receiver's identity or public key to obtain two shares of the receiver's private key. Using the two shares of the receiver's private key, the receiver may construct their own complete private key, which corresponds to the public key with which a message was encrypted. This portion of Boneh merely shows that a receiver may request private key shares from a plurality of private key generators, each having private a single private key share, and does not show or suggest producing an IBE public key of a sender as part of a decryption process, as required by claims 1 and 18.

There is nothing in the cited sections of Boneh, or in any other portion of Boneh, that shows or suggests that decrypting ciphertext produces an IBE public key of the sender ID_A that corresponds to an IBE private key SK_A, as required by claims 1 and 18. Boneh therefore fails to make up for the admitted deficiencies of Zheng. Claims 1 and 18 are therefore patentable over Zheng and Boneh, whether or not these references are combined as proposed in the Office Action. Claims 2-12 depend from claim 1 and are patentable because claim 1 is patentable. Claim 19 depends from claim 18 and is patentable because claim 18 is patentable.

Conclusion

The foregoing demonstrates that claims 1-19 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

Respectfully submitted,

Date: August 21, 2009

/David C. Kellogg/
David C. Kellogg
Reg. No. 62,958
Agent for Applicant
Customer No. 36532